TELKOMNIKA, Vol. 11, No. 7, July 2013, pp. 4151 ~ 4158
e-ISSN: 2087-278X

DWT Domain Information Hiding Approach Using Detail Sub-band Feature Adjustment

Qiudong Sun*, Ping Guan, Yongping Qiu, Wenying Yan
School of Electronic and Electrical Engineering, Shanghai Second Polytechnic University, Shanghai 201209, China
2360 Jinhai Road, Shanghai 201209, China, 86-21-50216895/86-21-50214979
*Corresponding author, e-mail: qdsun@sspu.cn

Abstract

In recent years, many algorithms based on HVS and DWT had been proposed for watermarking. But most of them aimed at the binary iconic watermark. So they are unsuitable for embedding other format watermarks such as the text file, the gray image or even the color image. This paper proposed a multi-format data source file supporting algorithm for watermarking and information hiding. Firstly, the algorithm transformed a source file into a binary watermark sequence and put redundant encoding and random scrambling on it. Then, the algorithm selected two neighboring blocks each time from the Hilbert scanning sequence of the host image blocks, and transformed them by DWT. Lastly, according to the different codes of each two sequential watermark bits, the algorithm chose one of two thresholds of just noticeable difference (JND) to modify the average value features of two corresponding detail sub-bands to insert the watermark into the host image. Extracting hidden information only to need the embedded image without the original host images and the data source file, implemented the blind extraction to improve the security of secret information. The experimental results show that the embedded watermark is invisible, and the algorithm is robust to common image processing operations.

Keywords*: information hiding, multi-format watermarks, just noticeable difference, wavelet transformation, detail sub-band feature encoding*

1. Introduction

For many years, people had made a lot of works for the security of multimedia information transmission: such as scrambling technique, watermarking technique, hiding technique and so on [1]-[15]. For an effective watermarking method, three basic requirements should be satisfied: transparency, robustness and security. The former two are in conflict with each other. To dissolve this conflict availably, we can consider using the masking characteristic of human visual system (HVS) [1]. Generally, the watermarking algorithm works in spatial domain or in transform domain (such as DWT). The latter is more desirable, because it has better performance. A good watermarking technique also should extract the watermark from embedded-image blindly.

In recent years, many algorithms based on HVS and DWT had been proposed for watermarking [1]-[12]. Some of them [1]-[4] had also implemented the blind extraction. But most of them aimed at the binary iconic watermark. So they are unsuitable for embedding other format watermarks such as the text file, the gray image or even the color image.

In this paper, we propose an adaptive watermarking method based on average value relation of corresponding DWT sub-bands of two neighboring blocks with double JND thresholds, which supports embedding multi-format watermarks. As mentioned previously, in order to adjust the input image for transparent watermarks, we employ a visual model [2], [11] to calculate the different double block based JND thresholds for determining the intensity of watermarking at the different locations of image. We also give a redundant encoding method for robustness.

This paper is organized as follows: Section 2 gives the JND thresholds calculation equation and the adaptive watermarking theories. Section 3 presents the watermarking algorithm and its extraction in detail. Section 4 examines the performance of proposed algorithm, and shows that it yields more effective and better performance, both in terms of

Received February 18, 2013; Revised May 4, 2013; Accepted May 15, 2013

transparency and robustness through simulation. Section 5 gives the conclusion of the whole paper.

2. Adaptive Watermarking Principles

2.1. Just Noticeable Difference (JND)

If the $K \times K$ image block $\boldsymbol{B}_{uv}$ located at (u, v) is DWT-transformed into an approximate image and three detail sub-band images $\boldsymbol{D}'_{uv}$ ($s \in$ HH, HL, LH). The JNDs of three detail sub-bands are represented as follows [2], [11]:

$$\boldsymbol{J}_{uv}^{s} = \boldsymbol{T}_{uv} \boldsymbol{F}_{s} \tag{1}$$

where $\boldsymbol{T}_{uv}$ is the normalized value of $\boldsymbol{T}'_{uv}=f\gamma(f)\boldsymbol{E}_{uv}$ in the range of $[a, b]$, while $\boldsymbol{E}_{uv}$ is the normalized entropy of $\boldsymbol{B}_{uv}$. When $s \in$ HH, $\boldsymbol{F}_s$ equals 1.414, otherwise it is 1 [2], [11]. γ is the human eyes relative sensitivity, which can be approximated by the equation as follows [5]:

$$\gamma(f) = \frac{\Delta f}{f} = 0.02\left[e^{\frac{128}{f}-1} + e^{\frac{1}{(256-f)}-\frac{1}{128}} \right] \tag{2}$$

where f=mean($\boldsymbol{B}_{uv}$).

2.2. Watermark Embedding

If $\boldsymbol{B}_{uv1}$ and $\boldsymbol{B}_{uv2}$ are the two neighboring image blocks and their DWT-transformed detail sub-bands are $\boldsymbol{D}^{s}_{uv1}$ and $\boldsymbol{D}^{s}_{uv2}$ (simply marked by $\boldsymbol{D}_t$, $t \in \{1, 2\}$). Now we can define the admissible distortion factor of sub-band coefficients of DWT as follows:

$$\lambda_t = \frac{|\boldsymbol{D}_t| + \delta}{\text{mean}(|\boldsymbol{D}_t|) + \delta} \qquad t \in \{1, 2\} \tag{3}$$

where δ is a positive number, which is a effect factor of absolute values of detail sub-band coefficients to embedding intensity.

We assume that μ is the mean value of JNDs of two neighboring blocks. It is represented by equations as follows:

$$\mu = \frac{1}{2}\left(\boldsymbol{J}_{uv1}^{s} + \boldsymbol{J}_{uv2}^{s}\right) \tag{4}$$

If the normalized range of $[a, b]$ in equation (1) is set by two different un-overlapped ascend ranges $[a_0, b_0]$ and $[a_1, b_1]$, such as [1, 2] and [6, 7], then we can get two different $\mu \cdot \cdot$ from equation (1) and (4). They can be represented by μ_r, $r \in \{0,1\}$.

We also assume that $\boldsymbol{W}$ is a watermark sequence, Δd is the corresponding DWT detail sub-band coefficients difference of two neighboring blocks at same direction, and $\varepsilon \cdot$ is the adjustment intensity matrix of detail sub-bands coefficients. They are represented by equations as follows respectively:

$$\Delta d = \text{Sign}(\boldsymbol{W}_k)[\text{mean}(\boldsymbol{D}_2) - \text{mean}(\boldsymbol{D}_1)] \tag{5}$$

$$\varepsilon_t = \frac{1}{2}\text{Sign}(\boldsymbol{W}_k + t)\lambda_t\left(\mu_{\boldsymbol{W}_{k+1}} - \Delta d\right) \tag{6}$$

where Sign(•) is a sign function, $\boldsymbol{W}_k$ is the k-th element of binary watermark sequence $\boldsymbol{W}$.

Table 1. Relationship between watermark codes and DWT detail sub-band features of two neighboring blocks

$\boldsymbol{W}_k$ and $\boldsymbol{W}_{k+1}$	The value relationship of corresponding DWT detail sub-bands
00	$\text{mean}(\boldsymbol{D}_2') - \text{mean}(\boldsymbol{D}_1') = \mu_0$
01	$\text{mean}(\boldsymbol{D}_2') - \text{mean}(\boldsymbol{D}_1') \geq \mu_1$
10	$\text{mean}(\boldsymbol{D}_2') - \text{mean}(\boldsymbol{D}_1') = -\mu_0$
11	$\text{mean}(\boldsymbol{D}_2') - \text{mean}(\boldsymbol{D}_1') \leq -\mu_1$

If the DWT detail sub-band features of two neighboring blocks after embedded should be satisfied the relationship with two sequential bits $\boldsymbol{W}_k$ and $\boldsymbol{W}_{k+1}$ of watermark sequence as shown in Table 1. We can prove that the watermark embedding rule is as follows:

$$\boldsymbol{D}_t' = \begin{cases} \boldsymbol{D}_t + \varepsilon_t & \text{if } (\boldsymbol{W}_{k+1} = 1 \text{ and } \Delta d < \mu) \text{ or } (\boldsymbol{W}_{k+1} = 0) \\ \boldsymbol{D}_t & \text{otherwise} \end{cases} \tag{7}$$

From above, we know that the watermark embedding capacity of this algorithm can reach to the value of $(3MN)/K^2$ bits. So it is enough to ensure the watermark's robustness.

2.3. Watermark Extraction

The watermark extracting should select two neighboring blocks $\boldsymbol{B}'_{uv1}$ and $\boldsymbol{B}'_{uv2}$ each time from Hilbert scanning sequence of embedded-image blocks, and a couple of their DWT detail sub-bands $\hat{\boldsymbol{D}}_1$ and $\hat{\boldsymbol{D}}_2$. And set $th=(b_0+a_1)/2$. Then, the watermark extraction rule can be proved as follows:

$$\hat{\boldsymbol{W}}_k = \begin{cases} 0, & \text{if } \text{mean}(\hat{\boldsymbol{D}}_2) \geq \text{mean}(\hat{\boldsymbol{D}}_1) \\ 1, & \text{otherwise} \end{cases} \tag{8}$$

$$\hat{\boldsymbol{W}}_{k+1} = \begin{cases} 0, & \text{if } \left[\text{Sign}(\boldsymbol{W}_k)\left(\text{mean}(\hat{\boldsymbol{D}}_2) - \text{mean}(\hat{\boldsymbol{D}}_1)\right)\right] < th \\ 1, & \text{otherwise} \end{cases} \tag{9}$$

From equation (9), we know that the anti-interference ability of this algorithm lies on the gap between b_0 and a_1. The larger this gap is, the better the anti-interference ability is.

3. Watermarking Algorithm

3.1. Embedding Algorithm

The steps of embedding algorithms are as follows:

Step 1: Convert a watermark file into a bit stream $\boldsymbol{W}$, which is called the original watermark.

Step 2: Append some zeros to the end of $\boldsymbol{W}$, and enable its length to just equal to 4.5 times of total blocks number of host image.

Step 3: To improve the robustness of watermarking and assure its redundancy, the original watermark $\boldsymbol{W}$ should be extended periodically as follows:

$$\boldsymbol{W}_{\text{ex}}^m = \boldsymbol{W}_l \quad m = n \cdot L + l; n = 0,1,\cdots,Cr-1; l = 0,1,\cdots,L-1 \tag{10}$$

where $\boldsymbol{W}_{\text{ex}}$ is the extended watermark, $\boldsymbol{W}_{\text{ex}}^m$ represents its m-th element, Cr is the extended factor.

Step 4: To improve the security of watermarking, $\boldsymbol{W}_{\text{ex}}$ should be scrambled randomly [13].

Step 5: To keep the relativity of two neighboring image blocks, the original host image $\boldsymbol{I}$ can be scanned by Hilbert scanning to obtain a Hilbert scanning sequence.

Step 6: Select two neighboring image blocks $\boldsymbol{B}_{uv1}$ and $\boldsymbol{B}_{uv2}$ each time from the Hilbert scanning sequence, and embed the watermark according to the method as mentioned in section 2 until the tree couple of DWT detail sub-bands of all blocks have been processed.

Step 7: After applied the inverse DWT for all watermark embedded blocks, an embedded-image $\boldsymbol{I}'$ can be obtained.

3.2. Extracting Algorithm

The steps of extracting algorithms are as follows:

Step 1: Scan the embedded-image $\boldsymbol{I}'$ by Hilbert scanning as the same order as that in embedding.

Step 2: Select two neighboring image blocks $\boldsymbol{B}'_{uv1}$ and $\boldsymbol{B}'_{uv2}$ each time from the Hilbert scanning sequence, and extract the watermark according to the method as mentioned in section 2 until the tree couple of DWT detail sub-bands of all blocks have been processed.

Step 3: After that, we can get a watermark sequence $\hat{\boldsymbol{W}}_{\text{ex}}$, which involves the Cr copies of recovered watermark.

Step 4: If there was a scrambling when watermark was embedded, here we should do unscrambling [13] to $\hat{\boldsymbol{W}}_{\text{ex}}$.

Step 5: The final watermark can be obtained from $\hat{\boldsymbol{W}}_{\text{ex}}$ as follows:

$$\hat{\boldsymbol{W}}_l = \begin{cases} 1, & \text{if } \sum_{n=0}^{Cr-1} \hat{\boldsymbol{W}}_{\text{ex}}^{n \cdot L+l} \geq \dfrac{Cr}{2} \\ 0, & \text{else} \end{cases} \tag{11}$$

Step 6: The binary watermark sequence $\hat{\boldsymbol{W}}$ should be converted back into a file as the same format as that in original source.

4. Simulation Results and Analysis

The peak signal to noise ratio (PSNR) is employed to evaluate the quality of embedded-image, and the bit error rate (BER) is employed to evaluate the quality of extracted watermark, meanwhile the normalized correlation coefficient (ρ) □ between the extracted watermark and the original one is employed to evaluate the quality of watermarking technique.

4.1. Influence of Parameters on Algorithm Performance

In the experiment, the proposed algorithm was evaluated on the gray image "Lena" (512×512). The block size K can be 8, 4 or 2. In order to ensure the anti-interference ability of algorithm, [a_0, b_0] should be set with a smaller range and [a_1, b_1] should be set with a bigger range. So we set [a_0, b_0]=[1,2]. Figure 1 is the relationship between PSNR of embedded-image and the effect factor δ at different block sizes. Figure 2 is the relationship between BER of the extracted watermark and δ. Figure 3 is the relationship between PSNR and the JND normalized range [a_1, b_1] at full embedding capacity.

As shown in Figure 1, the PSNRs of embedded-image are constant when K =2 (not recommended because of its low PSNR), but when K >2, the bigger δ is, the higher PSNRs are. But the bigger δ will decrease the embedding intensity, it leads that the performance of extracting algorithm will be worse, especially when K =8, the BERs will be higher. As shown in Figure 2, we know that BERs are always zeros when δ ≤1, and whatever the K is. So we set the δ=1 in the following experiments. As shown in Figure 3, the PSNRs are almost in inverse proportion to [a_1, b_1]. The smaller [a_1, b_1] is, the higher PSNRs are, and the better imperceptibility of embedded watermark is. So, an appropriate range [a_1, b_1] is better. Here, we set [a_1, b_1]=[6,7].

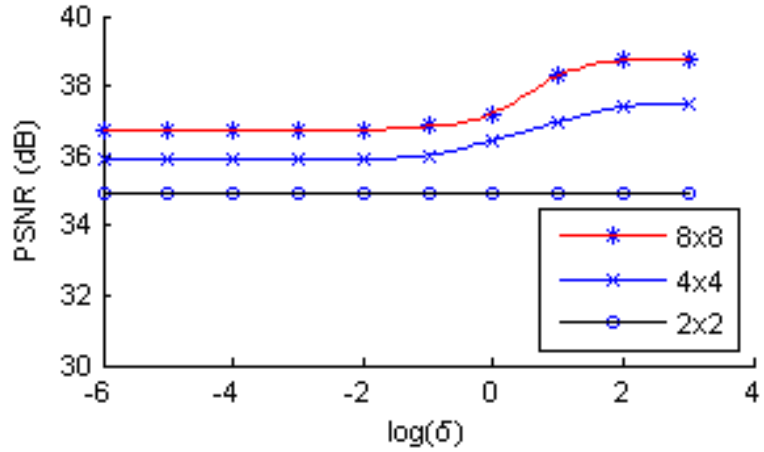

Figure 1. Relationship between PSNR and δ

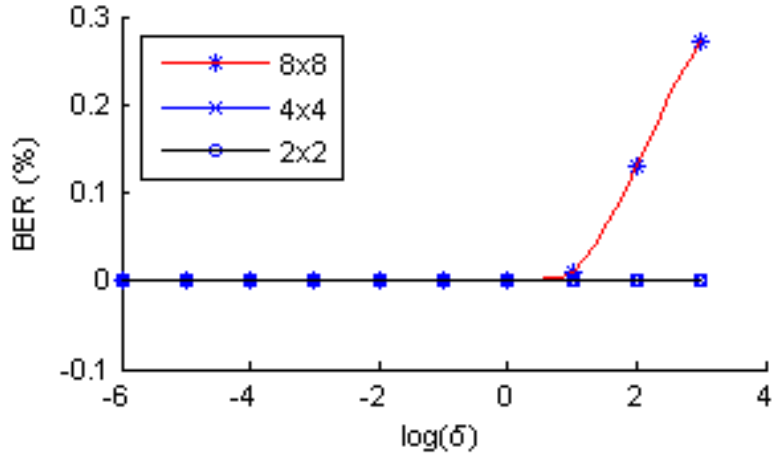

Figure 2. Relationship between BER and δ

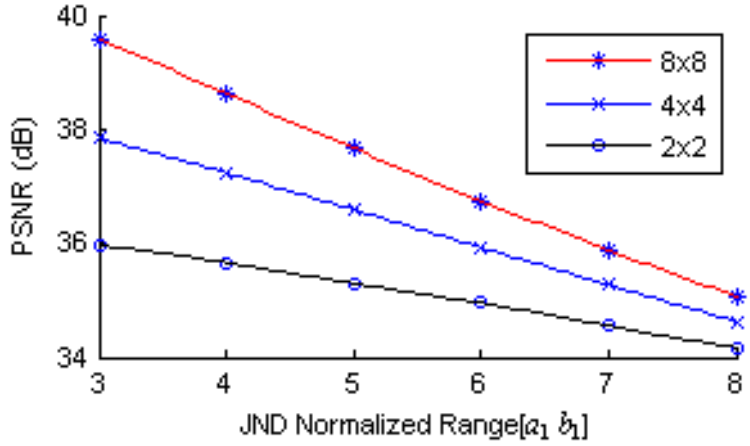

Figure 3. Relationship between PSNR and a_1 ($[a_0, b_0]$=[1,2], b_1=a_1+1)

4.2. Multi-format Watermarking Results

Figure 4(a) is the original image of "Lena". Figures 4(b), (d), (f) and (h) are four type watermarks, which are 32×32 binary image, 32×32 color image, 64×64 gray image and text file respectively. Figures 4(c), (e), (g) and (i) are their watermarking results to Figure 4(a) when K =4, and their PSNRs are 36.0dB, 36.7dB, 36.8dB and 37.2dB respectively. As shown in Figure 4, due to being converted into a binary sequence finally, the watermarks with different format and size can be embedded into the host image with the same way and their PSNRs are almost same. In addition, considering the visual perception in the algorithm, the various watermarks in different embedded-images are all invisible. The algorithm can rightly extract the watermarks from the embedded-images.

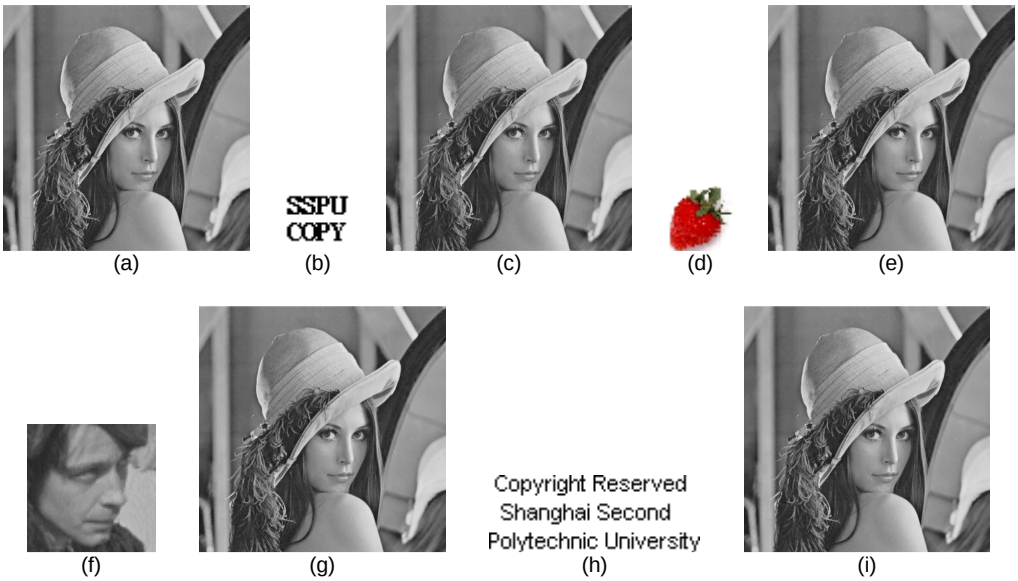

Figure 4. Watermarking Results of "Lena"

4.3. Performance Variety on Scrambling and Various Attacks

In the experiment, all attack items are operated on Photoshop 6.0, besides the JPEG compression and central region cropping. Figure. 5 is the binary image watermarking results of the proposed algorithm acting on the gray image "Lena" when K=4. The original binary watermark image is as shown in Figure 4(b). Figure 5(a)~(h) are the recovered copies from the watermarked image by attack of cropping the central region with size 300×300, JPEG compression with 85% quality, contrast enhancement with 70%, brightness enhancement with 100%, adding Gaussian noise with 3%, adding salt and pepper noise with 3%, eddy distortion with 10 degree and 10 times edge enhancement respectively. Figure 5(i)~(p) are the recovered results under the same condition as Figure 5(a)~(h) respectively but putting the scrambling on watermark. As shown in Figure 5, the watermarking algorithm is robust against the general image processing and the performance is better when there is scrambling on watermark.

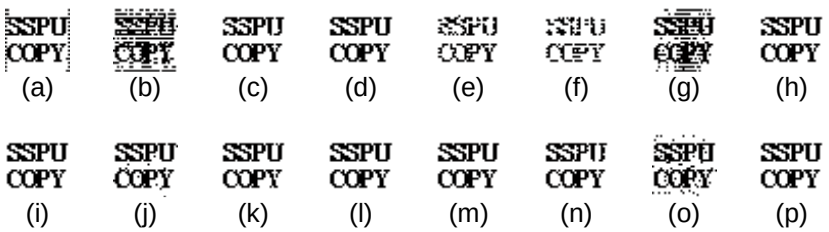

Figure 5. Extracted Watermarks under Various Attacks

4.4. Comparison of Text Watermarking with Binary Image Watermarking

Under the condition of scrambling, we also give the zero BER tests of attack defense of text watermarking and its performance comparison with that of binary image watermarking. As shown in Table II, the robustness of text watermarking and that of binary image are both good. But obviously the former has better performance than the latter, because it has more redundancy at the same condition.

Table 2. The zero BER attack defence tests of text watermarking and its comparison with that of binary image

The Normalized Correlation Coefficient ρ				
Attack items	Text ("SSPU COPY")		Binary image (As shown in Figure 5)	
	K=8	K=4	K=8	K=4
Brightness enhancement (100%)	1	1	0.998	1
Contrast enhancement (60%)	1	1	0.990	1
Edge enhancement (10times)	1	1	0.960	1
Extrusion distortion (4%)	1	1	0.796	0.967
Eddy distortion (7°)	1	1	0.747	0.924
Add Gaussian noise (3%)	1	1	0.998	0.988
Add uniformity noise (5%)	1	1	0.995	0.995
Add salt & pepper noise (1%)	1	1	0.980	1
Cropping in central region (256×256)	1	1	0.998	1
JPEG compression (90% quality)	1	1	1	1

5. Conclusion

This paper presented a new watermarking and information hiding algorithm based on DWT detail sub-band feature encoding for multi-format watermarks. In our approach, the comparability of corresponding DWT detail sub-bands of two neighboring image blocks was considered, and in order to improve the transparency of watermarking, the visual model was also used for determining the embedding intensity in different regions with different textures. In addition, in order to defense the general image processing attacks, the redundant encoding was given for increasing the embedded copies of watermark, and the scrambling was given for improving its robustness and security. The experiment results demonstrated that the proposed algorithm yields the acceptable performance for transparency and robustness to general image attacks and the text watermarking with scrambling has a better performance than that of binary image.

Acknowledgement

This work was supported by a grant from the Technological Innovation Foundation of Shanghai Municipal Education Commission (No. 09YZ456) and the Key Disciplines of Shanghai Municipal Education Commission (No. J51801).

References

[1] Barni M, Bartolini F, Piva A. Improved Wavelet-based Watermarking Through Pixel-wise Masking. *IEEE Transactions on Image Processing*. 2001; 10(5): 783-791.
[2] Yang HF, Chen XW. A Robust Image-adaptive Public Watermarking Technique in Wavelet Domain. *Journal of Software*. 2003; 14(9): 1652-1660.
[3] Cao JG, Fowler JE, Younan NH. *An Image-adaptive Watermark Based on a Redundant Wavelet Transform*. IEEE International Conference on Image Processing. Thessaloniki. 2001; 2: 277-281.
[4] Yang CY. Robust Reversible Data Hiding Scheme Based on Integer Wavelet Transform. *ICIC Express Letters*. 2011; 5(11): 4209-4214.
[5] Stuti B, Sachin M, Anand M, Surya PS. An Improved Algorithm for Data Hiding Using HH-subband Haar Wavelet Coefficients. *International Journal of Advancements in Computing Technology*. 2010; 2(2): 109-116.
[6] Zhang T, Mu DJ, Ren S. Information Hiding (IH) Algorithm Based on Gaussian Pyramid and GHM (Geronimo Hardin Massopust) Multi-wavelet Transformation. *International Journal of Digital Content Technology and its Applications*. 2011; 5(3): 210-218.

[7] Zheng W, Zhao ZG. *Wavelet Domain Digital Image Hiding Algorithm Based on CNN Encryption*. Proceedings of 2010 International Conference on Computer Application and System Modeling (CCASM 2010). Taiyuan. 2010; 8: 386-390.
[8] Huang HY, Chang SH. *A Lossless Data Hiding Based on Discrete Haar Wavelet Transform*. Proceedings of 10th IEEE International Conference on Computer and Information Technology (CIT-2010), 7th IEEE International Conference on Embedded Software and Systems. Changsha. 2010: 1554-1559.
[9] Gunjal BL, Manthalkar RR. *Discrete Wavelet Transform Based Strongly Robust Watermarking Scheme for Information Hiding in Digital Images*. Proceedings of 3rd International Conference on Emerging Trends in Engineering and Technology (ICETET). Goa. 2010: 124-129.
[10] Wang ZM, Zhang YJ, Wu JH. A Wavelet Domain Watermarking Technique Based on Human Visual System. *Journal of Nanchang University (Natural Science)*. 2005; 29(4): 400-403.
[11] Sun QD, Ma WX, Yan WY, Dai H. Text Encryption Technique Based on Robust Image Watermarking. *Journal of Image and Graphics*. 2008; 13(10): 1942-1946.
[12] Wu LY, Yang F. An Improved Digital Watermarking Algorithm Based on DWT. *Control and Automation*. 2007; 23(6.3): 46-47.
[13] Sun QD, Ma WX, Yan WY, Dai H. A Random Scrambling Method for Digital Image Encryption: Comparison with the Technique Based on Arnold Transform. *Journal of Shanghai Second Polytechnic University*. 2008; 25(3): 159-163.
[14] Zhang Y, Xia JL, Cai P, Chen B. Plaintext Related Two-level Secret Key Image Encryption Scheme. *TELKOMNIKA*. 2012; 10(6): 1254-1262.
[15] Chen GX, Zhang PC, Zhang M, Wu YL. Batch Zero-steganographic Model for Graph Transformation. *TELKOMNIKA*. 2012; 10(4): 734-742.